Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Wireless E911 Location Accuracy Requirements	)	PS Docket No. 07-114
	)	
	)	
	)	
	)	

Comments of ADT LLC d/b/a ADT Security Services

ADT LLC d/b/a ADT Security Services ("ADT") submits these comments in response to the Fourth Further Notice of Proposed Rulemaking in the above-captioned proceeding.[1] ADT specifically responds to the request for comment regarding the appropriate privacy and security framework for z-axis data.[2] For the reasons set forth below, the Federal Communications Commission ("Commission") should confirm that neither its existing rules, nor any privacy rules adopted in this proceeding, preclude or otherwise impair the ability of CMRS carriers to provide location information to entities, such as ADT, for providing public safety services and emergency response outside of "responding to 911 calls." It is in the public interest to ensure that public safety monitoring companies are able to use that information in providing their public safety-related services.

[1] *Wireless E911 Location Accuracy Requirements*, Fourth Further Notice of Proposed Rulemaking, PS Docket No. 07-114 (rel. March 18, 2019) ("*Notice*").
[2] *Id.* at ¶ 29. To assist first responders in locating cellphone callers in multi-story buildings, the *Notice* proposes a vertical or z-axis location metric of plus or minus 3 meters from the handset for 80% of indoor wireless E911 calls pursuant to a phased schedule. *Id*. at ¶ 11. The Commission has previously established indoor location horizontal x/y geo-coordinates accurate to within 50 meters as one alternative for heightened indoor location accuracy. *Wireless E911 Location Accuracy Requirements*, Fourth Report and Order, PS Docket No. 07-114, 30 FCC Rcd 1259, 1287 ¶ 74 (rel. February 3, 2015) ("*Indoor Location Fourth Report and Order*").

ADT's Use of Location Data for Public Safety Services

The *Notice* correctly observes that cellphones and smartphones "have become an indispensable tool to protect consumers' health, property and wellbeing."[3] As the nation's largest alarm monitoring services provider, ADT is leveraging this technology to extend its public safety services beyond the home. ADT uses location data for its public safety services in a variety of important ways that are outside of "responding to 911 calls."

Last year, for example, ADT launched ADT Go, a location-based mobile application that can be downloaded to any Android or iOS smart phone. ADT Go enables family and friends to form a "circle" through which they can, with their consent and authorization, share their location, and other information, with each other. ADT Go also uses real-time GPS data to pinpoint the location of the user in the event of an automobile accident or other emergency. And, ADT Go includes an SOS Button that, when depressed and held, connects to an ADT agent that can provide rapid assistance as warranted by the situation, including calling the Public Safety Answering Point ("PSAP") to dispatch emergency personnel to the location.

ADT also leverages wireless mobile technology to provide our customers with an ADT-owned mobile medical alert device that can be used to summon family members, caretakers, or first responders in the event of a fall or other medical emergency. As with the SOS Button, ADT customers can push a button on their ADT device to reach one of our agents who can dispatch specified contacts or emergency personnel. Our devices also have fall detection capabilities that can automatically send an alert if a fall occurs. These ADT devices run over a wireless mobile network through ADT's relationship with one of the national wireless carriers. ADT uses a variety of methods to identify a customer's location, including technology embedded in the device itself, and other tools provided by its wireless carriers.

[3] *Notice* at ¶ 1.

The NEAD Privacy and Security Plan

As the Commission has long recognized, identifying the location of a wireless caller can be challenging, particularly in indoor environments where most wireless calls originate. To further meet this challenge, the Commission adopted enhanced indoor wireless location rules in its 2015 *Indoor Location Fourth Report and Order*. There, the Commission required CMRS carriers to either provide a dispatchable location, defined as a street address and floor, office or room number, or to convey horizontal x/y geo-coordinates that can locate the device within 50 meters using a variety of location technologies.[4] The order also called for the establishment of a vertical or z-axis but did not adopt a specific z-axis standard, which is the central thrust of this *Notice*.

To support the ability to provide a dispatchable location, identified as the "gold standard" for location information, the Commission also established the National Emergency Address Database ("NEAD").[5] The NEAD is a database of Wi-Fi media access control (MAC) addresses and Bluetooth Public Device Addresses (BT-PDA) that will enable wireless providers to obtain a precise indoor location of a caller making a 911 call. Upon the initiation of a 911 call, the wireless device would obtain nearby MAC or Bluetooth reference points that the wireless carrier could then look up in the NEAD for dispatchable location information. Given the potentially sensitive information contained in the NEAD, the Commission directed stakeholders to devise a privacy and security plan. The plan was submitted on February 3, 2017 and approved by the Commission.[6]

[4] *Indoor Location Fourth Report and Order*, 30 FCC Rcd at 1261, ¶ 6.
[5] *Indoor Location Fourth Report and Order*, 30 FCC Rcd at 1274, ¶ 44.
[6] *Wireless E911 Location Accuracy Requirements*, Memorandum Opinion and Order, 32 FCC Rcd 9699 ¶ 1 (2017).

The *Notice* references this plan and seeks comment on its applicability to z-axis location information.[7] Specifically, it notes the Commission's requirement that "as a condition of using the NEAD or any information contained therein to meet our 911 location requirements, and prior to the use of the NEAD, CMRS providers must certify that they will not use the NEAD or associated data for any purpose other than for the purpose of responding to 911 calls, except as required by law."[8] The Commission asks whether z-axis data "should be limited to 911 calls except as otherwise required by law and if such limitation should be implemented and codified in a manner similar to the limitations applicable to the NEAD described above."[9] The *Notice* does not ask whether other geolocation information, such as the indoor x/y coordinates, should also be subject to the same privacy restrictions.

Wireless Providers Should Not be Precluded From Sharing Location Information for Public Safety Purposes Outside of 911 Calls

ADT fully appreciates the need to protect and secure sensitive personal information, including location information. The *Notice*, for example, cites to a letter from Public Knowledge recounting instances where wireless carriers may have indirectly provided access to location information to aggregators that ultimately was made available to bounty hunters or others.[10] The privacy concerns raised by such activities do not, however, justify a blanket ban on CMRS providers sharing location information critical for public safety purposes outside the context of their own customers making a 911 call. It is important for the Commission to recognize that protection of public safety is not limited to such 911 calls. To the contrary, services provided by alarm monitoring companies such as ADT are a vital component of the public safety ecosystem,

[7] *Notice* at ¶ 29.
[8] *Notice* at ¶ 29 (quoting *Indoor Location Fourth Report and Order*, 30 FCC Rcd at 1285 ¶ 71).
[9] *Id.*
[10] *Notice* at ¶ 29, n. 75 (citing Letter from Harold Feld, Senior VP, Public Knowledge, to Marlene H. Dortch, Secretary, PS Docket No. 07-114, FCC at 2 (filed March 12, 2019)).

as evidenced by the recent agreement to allow qualified alarm service companies to utilize FirstNet when notifying 911 call centers on their customers' behalf. [11]

Rules that prohibit CMRS providers from providing accurate and precise location information except in the specific instance of a direct 911 call would hamper the ability of ADT and other providers of public safety services to help protect their customers. As described above, ADT offers mobile public safety services that enable its customers to contact trained ADT agents in the event of a medical emergency, such as a fall or automobile accident, or where a customer feels threatened or otherwise needs assistance. ADT agents are able to assess the situation, and, where warranted, place a call to a PSAP or first responders. In other circumstances, the agent may contact a family member or obtain roadside assistance. It should go without saying that in such circumstances, ADT's customer wants to be located; which is why our customers agree to ADT's use of their location information for this purpose when enrolling in our service.

In such events, it is critical that ADT convey the location of its customer in distress, and in some instances it relies on the underlying CMRS provider to supply or supplement location information. This is particularly important if the ADT customer is located in a high rise building or other environment where the GPS capabilities embedded in ADT's devices may be impaired.[12] On February 14, 2018, Fernando Paz (an ADT employee) heard what no parent ever wants to hear: there was an active shooter at his daughter Lauren's school, Marjory Stoneman Douglas High in Parkland, FL. In all the confusion, the Paz family used ADT Go for the clearest communication. [13] Lauren was able to silently press the SOS button on the app, and, using the

[11] *See TMA to Support Alarm Companies Participation in FirstNet.* https://tma.us/tma-to-support-alarm-companies-participation-in-firstnet/ (last visited May 20, 2019).
[12] *See Indoor Location Fourth Report and Order*, 30 FCC Rcd at 1266-67 ¶ 19 (noting that "satellite-based location technologies do not provide accurate location data for many wireless calls placed from indoor locations, particularly in urban areas where a growing number of Americans reside.")
[13] https://www.adt.com/go (last visited May 20, 2019).

technology embedded in her cellular phone, her family was able to see that she was in a different building than the shooter. Unfortunately, z-access information was not available. In situations like this, having access to carrier-provided customer proprietary network information (CPNI) x,y, *and* z-axis location information could help ADT monitoring center employees more accurately convey customer information, including altitude or floor number, in addition to building address, to first responders in emergency situations.

ADT takes substantial precautions to protect the location information it receives, either directly or from a CMRS provider, and it uses location information as necessary to provide its public safety monitoring services, for example by sharing such information with "third-party emergency service providers such as police departments, fire departments, and emergency medical services."[14]

ADT uses CMRS location information in support of its public safety services and does not share that information for unrelated purposes, such as reselling to aggregators and third-party marketing. Because of the sensitivity of location information and general data privacy concerns, restrictions on sharing location information with aggregators or for marketing may be appropriate, but the FCC should not foreclose the sharing of location data for uses that advance and protect public safety more broadly than direct response to 911 calls.

ADT anticipates that the sharing of location information will go both ways. ADT is working with other vendors and communications service providers to make available information that it obtains as a result of its monitoring services. For example, in its comments regarding implementation of Kari's law and E911 for enterprise communications systems, ADT

[14] ADT's privacy policy states that: "We collect your location-based information as part our service(s) to identify your location for dispatching or sharing with emergency service providers. We will only share this information with third party services for the sole purpose of providing you our service(s). You may opt-out of location-based services at any time by editing the setting at the device level." ADT does not sell its customer's information "to third parties for their own marketing purposes." https://www.adt.com/about-adt/legal/privacy-policy (last visited May 20, 2019).

described ways to use its increasingly IP-enabled monitoring devices to provide location or real-time situational information to first responders.[15][16] ADT's efforts reflect the company's strong commitment to public safety and as a trusted partner for emergency services providers. ADT's efforts, however, could be hampered if other providers feel constrained in sharing location information by overly restrictive privacy policies.

CONCLUSION

The Commission should ensure that its commendable efforts to protect the privacy and security of sensitive location information do not preclude wireless providers from sharing such information with ADT and other providers of critical public safety services and should take action to ensure that CPNI location information is only shared for public safety purposes.

Respectfully submitted,

/s/ Michael Pryor
Michael H. Pryor
Brownstein, Hyatt, Farber, Schreck, LLP
1155 F Street NW, Suite 1200
Washington, DC 20004
Telephone: (202) 383-4706
MPryor@BHFS.com

Counsel for ADT LLC d/b/a ADT Security Services

[15] Comments of ADT LLC d/b/a ADT Security Services, PS Docket Nos. 18-261, 17-239 (filed December 10, 2018).

Holly Borgmann
Head of Government Affairs
ADT LLC d/b/a ADT Security Services
1501 Yamato Road
Boca Raton, FL 33431
Telephone: (562) 226-3484
HBorgmann@adt.com

May 20, 2019